Cisco Secure Workload（旧 Cisco Tetration）

目次

Cisco Secure Workload の概要

Q. Cisco® Secure Workload プラットフォームとは簡単に言うとどのようなものですか。

A. Cisco Secure Workload は、オンプレミスのデータセンターとパブリッククラウドの両方でコンピューティング インスタンスを保護するように設計されたハイブリッドクラウドのワークロード保護プラットフォームです。これらのコンピューティング インスタンスには、仮想マシン、ベアメタルサーバー、コンテナが含まれます。機械学習、動作分析、アルゴリズムアプローチを使用して、この包括的なワークロード保護戦略を提供します。このアプローチにより、効果的なマイクロセグメンテーション、動作分析を使用したセキュリティインシデントのプロアクティブな識別、ソフトウェア関連の脆弱性の特定による攻撃対象領域の縮小を実装することで、ラテラルムーブメントを封じ込めることができます。

Q. お客様から見て、なぜ Cisco Secure Workload プラットフォームが必要となるのでしょうか。

A. アプリケーションはあらゆる組織にとって重要なエンティティであり、アプリケーションをサポートするワークロードはデータセンターと 1 つ以上のパブリッククラウドで構成されるマルチクラウド環境に展開されています。お客様が直面する重要な課題の 1 つは、俊敏性を損なうことなくアプリケーション用のセキュアなインフラストラクチャを実現する方法です。今日でも、大半のデータセンターは従来の境界のみのセキュリティで設計されていますが、それでは不十分です。この課題に対処するには、新しいアプローチが必要です。Cisco Secure Workload は、この課題に多次元のワークロード保護アプローチを使用した包括的な方法で対処します。

Q. ワークロード保護が必要とされる理由は何ですか。

A. 最新のアプリケーション アーキテクチャの進化に伴い、数百または数千の相互に依存するアプリケーションによって、エンタープライズ データセンターの規模も複雑さも増大しています。これにより、East-West トラフィックの増加、アプリケーションの導入、仮想化、コンテナ化、セキュリティに対する脅威、クラウドへの移行など、複雑化がますます進んでいます。

組織は、重要なアプリケーションワークロードを保護するために、ラテラルムーブメントを最小限に抑え、攻撃対象領域を縮小し、侵害の兆候（IoC）をより迅速に特定する新しいアプローチの必要性に迫られています。Cisco Secure Workload は、ビッグデータテクノロジーを使用した包括的なプラットフォームであり、これらの要件すべてにすぐに対応できるソリューションを規模を問わずに単一のプラットフォームで提供します。

Q. Cisco Secure Workload の機能を簡単に説明してください。

A. Cisco Secure Workload プラットフォームが提供するすぐに使用可能なソリューションにより、ネットワーク セキュリティ チーム、セキュリティ運用チーム、アプリケーション所有者は次のことが可能です。

- アプリケーションのコンポーネント、通信、および依存関係を完全に可視化し、アプリケーション資産を保護するためのゼロトラストモデルを実装する。
- アプリケーションの動作に基づいてマイクロセグメンテーション ポリシーを自動で生成する。ビジネス要件に応じて既存のセキュリティポリシーを取り込むメカニズムも用意されています。
- マイクロセグメンテーション ポリシーをすべてのマルチクラウド ワークロードに一貫して適用してラテラルムーブメントを最小限に抑える。

- ソフトウェアの脆弱性やエクスポージャを特定して攻撃対象領域を減らす。
- IoC を迅速に検出できるようにプロセス動作の基準を設定して逸脱を特定する。

これらを実現するために、Cisco Secure Workload は、エージェントベースとエージェントレスの両方のアプローチを使用してテレメトリデータを収集し、ワークロードのコンテキストを把握し、一貫性のある分散型のゼロトラストのセグメンテーションポリシーを大規模に適用します。Cisco Secure Workload は、Cisco AnyConnect® および Cisco ISE（Identity Services Engine）とも統合して、ユーザーとエンドポイントのコンテキストをセグメンテーションポリシーに組み込みます。これにより、管理者は、ユーザー、ユーザーグループ、ユーザーの場所、またはその他のユーザー関連属性に基づいてアプリケーションアクセスを制限するポリシーを定義できます。

全体として、Cisco Secure Workload のマイクロセグメンテーション アプローチは、ゼロトラストのセグメンテーション制御により、データセンターまたはクラウド環境全体でワークロード間のラテラルムーブメントを封じ込めるのに役立ちます。

Q. 詳細はどこで確認できますか。

A. www.cisco.com/go/secureworkload を参照してください。

アーキテクチャとユースケース

Q. Cisco Secure Workload プラットフォームのソフトウェアアーキテクチャはどのようになっていますか。

A. 図 1 にアーキテクチャを示します。

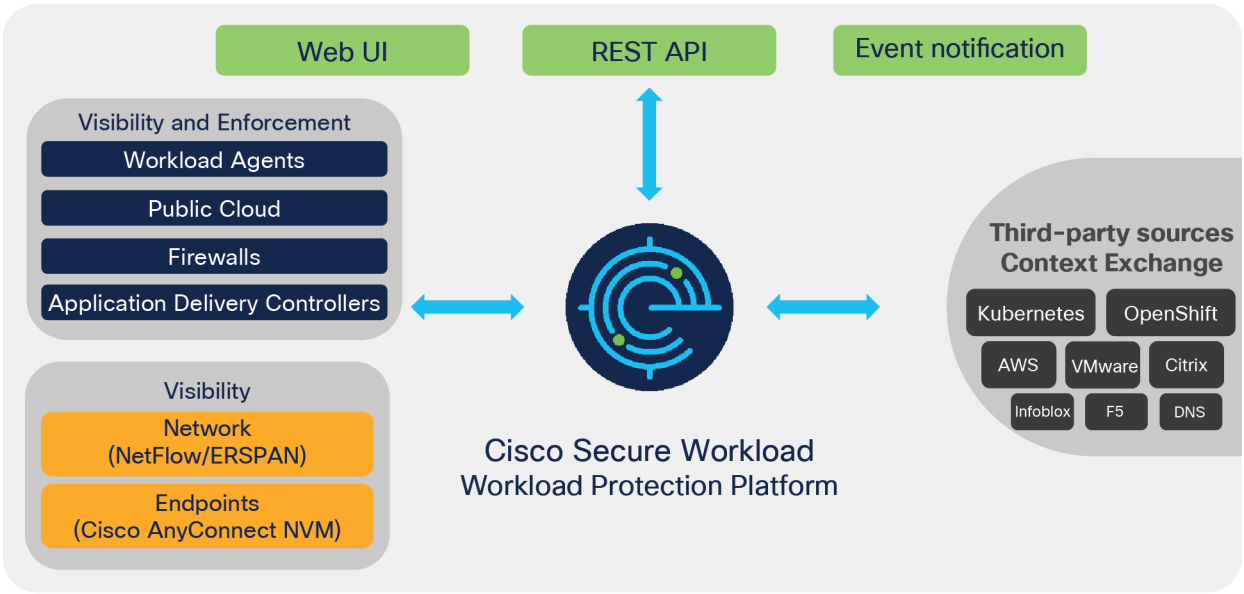

図 1.
Cisco Secure Workload のアーキテクチャ

Q. Cisco Secure Workload エージェントとは何ですか。

A. Cisco Secure Workload エージェントは、サーバーワークロード（仮想マシン、ベアメタル、またはコンテナホスト）にインストールされます。エージェントは、Linux、Microsoft Windows サーバー、Microsoft Windows デスクトップ、および IBM AIX 環境の主要なディストリビューションで使用できます。これらのエージェントは、すべての通信アクティビティ、プロセスデータ、ソフトウェアパッケージの詳細などのデータをワークロードから収集します。また、ネイティブのオペレーティングシステムのファイアウォールを直接制御して、マイクロセグメンテーション ポリシーの適用ポイントを提供します。

Q. AWS コネクタとは何ですか。

A. AWS コネクタは、お客様の Amazon Web Services クラウド環境との統合により、エージェントレス ワークロード セキュリティを提供します。提供される機能には、フローテレメトリ収集（VPC フローログ）、EC2 ワークロードインスタンスからのラベルおよびその他のメタデータ、エージェントレスポリシーの適用（セキュリティグループ）、および Elastic Kubernetes Service（EKS）からのワークロードメタデータの取り込みが含まれます。これにより、エージェントを展開することなく、AWS 環境に展開されたワークロードに対する完全な可視性と一貫したセグメンテーション アプローチが提供されます。

Q. Cisco Secure Workload フロー取り込みコネクタとは何ですか。

A. Secure Workload Ingest 仮想アプライアンスに導入された Cisco Secure Workload は、NetFlow/IPFIX やアプリケーション デリバリ コントローラ（ADC）とファイアウォール（Cisco 適応型セキュリティアプライアンス（ASA）/Cisco Secure Firewall Firepower® Threat Defense（FTD））などのネットワークデータソースと Cisco AnyConnect Network Visibility Module（NVM）などのエンドポイントデータソースを含む、幅広いテレメトリソースをサポートします。

Q. NetFlow コネクタとは何ですか。

A. NetFlow コネクタは、NetFlow v9 または IPFIX レコードから Cisco Secure Workload テレメトリデータを生成するように設計されています。NetFlow v9 とその標準化されたバリアントである IPFIX は、ルータやスイッチ、アプリケーション デリバリ コントローラ（ADC）、ファイアウォールなど、さまざまなネットワーキングデバイスからのフロー情報を提供します。NetFlow および IPFIX 対応デバイス（フローエクスポータ）は、パケットのローカル処理を実行して一連のフローレコードを作成し、コレクタインスタンスとして NetFlow コネクタに送信します。

Q. ERSPAN コネクタとは何ですか。

A. これらのアウトオブバンドのセンサーは、Encapsulated Remote SPAN（ERSPAN）設定を介してネットワーク インフラストラクチャから配信されるネットワーク パケット ヘッダーのコピーを使用して Cisco Secure Workload テレメトリデータを生成するように設計されています。これらのパケットヘッダーは、切り捨てられたトラフィックストリームとして仮想アプライアンスで実行されている ERSPAN センサーに配信されます。これらの ERSPAN センサーは、ERSPAN ヘッダーを削除し、元のパケットヘッダーデータを処理して Cisco Secure Workload テレメトリデータを生成します。このアプローチを使用して、ソフトウェアエージェントを展開できないネットワーク部分に可視性を拡張できます。

Q. ADC コネクタとは何ですか。

A. F5 BigIP や Citrix NetScaler などのアプリケーション デリバリ コントローラ（ADC）は、クライアント/サーバー接続の L4-L7 ステートフル転送への直接の関与を通じて IPFIX データを ADC コネクタに供給できます。この ADC フローデータは、Cisco Secure Workload フローテレメトリのソースとしてフロースティッチングの追加のコンテキストも提供し、運用の可視性に役立つコンテキストを提供します。また、ADC はアプリケーションサービスを提供するワークロードに対するポリシーの適用もサポートし、エージェントを展開できない特定のネットワーク部分に可視性とポリシー適用の両方を拡張します。

Q. Cisco ASA コネクタとは何ですか。

A. Cisco ASA および FTD ファイアウォールは、NetFlow セキュアイベントロギング（NSEL）の形式で NetFlow v9 をサポートします。ASA コネクタは、Cisco Secure Workload フローテレメトのリソースとして処理するために NSEL データを収集します。NSEL は、トラッキング対象のすべてのフローについての状態変更イベントや重要なステータスイベント（flow-create、flow-teardown、flow-denied など）をエクスポートするステートフルな IP フロートラッキング方式を提供します。また、従来の NetFlow と同様に、定期的な flow-update イベントを生成してフローの期間の定期的なバイトカウンタを提供します。

Q. Cisco AnyConnect コネクタとは何ですか。

A. Cisco AnyConnect コネクタは、ラップトップ、デスクトップ、スマートフォンなどのエンドポイントデバイスで実行されている Cisco AnyConnect エージェントから Network Visibility Module（NVM）テレメトリを収集するように設計されています。このテレメトリデータは、主に次の 2 つの目的で Cisco Secure Workload プラットフォームに取り込まれます。

1. ユーザーアクティビティと保護されているビジネスアプリケーションとの通信を可視化する
2. マイクロセグメンテーション ポリシーを拡張してユーザーとデバイスのコンテキストを含め、それに基づいてアプリケーションへのアクセスを許可または制限する

Q. Cisco Identify Services Engine（ISE）コネクタとは何ですか。

A. Cisco Secure Workload は、PxGrid からのリアルタイムのコンテキストフィードに登録する ISE コネクタを介して Cisco ISE と統合されます。このコンテキストには、ユーザーとグループの情報、エンドポイントプロファイル、デバイスポスチャ、および送信元グループタグ（SGT）が含まれます。これらにより、ユーザー/エンドポイント固有のルールを使用した動的なポリシーの定義と適用が可能になり、ワークロードポリシーの制御を強化および拡張できます。

Q. Cisco Secure Workload プラットフォームからユーザーは情報にどのようにアクセスしますか。

A. Cisco Secure Workload では、ナビゲーションしやすいスケーラブルな Web UI を介したユーザーアクセスと幅広い Representational State Transfer（REST）API を使用したプログラムによるアクセスが可能です。また、ノースバウンドシステムがポリシーの遵守違反やフローの異常などに関する通知を受け取れる Kafka ベースのプッシュ通知も用意されています。設定可能なアラートオプションとして、syslog、電子メール、Slack、Kinesis、PagerDuty などがあります。

Q. このアプローチではビッグデータと分析を活用していますか。

A. はい。ビッグデータ分析を使用しています。ビッグデータ分析を使用しないと、ワークロードセキュリティのユースケースに対応するために必要な速度と規模を実現することはできません。これらのアドバンスドテクノロジーによって、すぐに利用できるユースケースに対応しています。したがって、このプラットフォームを運用するために高度な分析機能は必要ありません。ビッグデータはテクノロジーにフォーカスしています。このプラットフォームはユースケースにフォーカスしています。

Q. Cisco Secure Workload プラットフォームはどのようなユースケースに対応していますか。

A. このプラットフォームは次のユースケースをサポートしています。

- **アプリケーションの動作情報：**アプリケーション コンポーネントとその詳細な依存関係を識別します。
- **マイクロセグメンテーション ポリシーの自動生成：**アプリケーションの依存関係に基づいて、一貫したマイクロセグメンテーション ポリシーを生成します。
- **ポリシーの自動適用：**異種環境に一貫したポリシーを適用することで効果的なアプリケーション セグメンテーションを実現します。このセグメンテーションによってゼロトラスト管理とラテラルムーブメントの抑制が可能になります。
- **ポリシーの遵守：**ポリシー違反を数分で検出し、アプリケーションポリシーを確実に遵守します。
- **プロセス動作の基準と逸脱：**プロセスハッシュ情報とともに完全なプロセスインベントリを収集し、動作の基準を設定し、逸脱を特定します。
- **ソフトウェアインベントリと脆弱性の検出：**サーバーにインストールされているすべてのソフトウェアパッケージとバージョンを特定します。Common Vulnerabilities and Exposures（CVE）データベースと追加のデータフィードを使用して、関連する脆弱性やエクスポージャがあるかどうかを検出し、アクティブなエクスプロイトから保護するためのアクションを実行します。
- **フォレンジック分析：**ワークロードの異常な動作や悪意のある動作を侵害の兆候として最大限の粒度で検出し、フォレンジック分析に活用します。

Q. Cisco Secure Workload はマイクロセグメンテーション以外にワークロードセキュリティのどのようなユースケースに対応していますか。

A. Cisco Secure Workload は、マイクロセグメンテーションに加えて、多次元のワークロード保護機能を提供します。これにより、ワークロードの攻撃対象領域が縮小されるだけでなく、オペレーティングシステムのプロセスレベルまで可視性が拡張され、より詳細なフォレンジックモニタリングが可能になります。詳細を次に示します。

- **サーバープロセスの基準と動作の逸脱：**Cisco Secure Workload は、それぞれのサーバーで実行されているプロセスの詳細を収集し、基準を設定します。この情報には、プロセス ID、プロセスパラメータ、それに関連するユーザー、プロセスの開始時刻、およびプロセスハッシュ（シグネチャ）が含まれています。プラットフォームは、良性およびフラグ付きの既知のプロセスハッシュで構成される最新のプロセスハッシュ判定フィードを維持し、ワークロード間でプロセスハッシュを比較して異常を検出します。特定のプロセスを実行しているサーバーまたはプロセスハッシュ情報を検索し、サーバーで実行されているすべてのプロセスのツリービュー スナップショットを取得できます。Cisco Secure Workload プラットフォームには、動作パターンの変更を追跡し、マルウェアの動作パターン（たとえば、特権昇格後に実行されるシェルコードなど）の類似点を検出するためのアルゴリズムがあります。Cisco Secure Workload では、このような動作の

逸脱に関するセキュリティイベントが発生します。セキュリティ運用チームは、定義が簡単なルールを使用して、それらのイベント、そのシビラティ（重大度）、および関連するアクションをカスタマイズできます。この情報を使用して、IOC を迅速に特定して修復手順を実行し、影響を最小限に抑えます。

- **ソフトウェアのインベントリと脆弱性の検出：**Cisco Secure Workload プラットフォームは、すべてのワークロードについて、インストールされているソフトウェアパッケージ、パッケージバージョン、パッチレベルなどの基準を設定します。プラットフォームは、NIST および OS ベンダーのデータパックを含む複数のソースからの最新の CVE データフィードを維持します。これには、脆弱性とエクスポージャの最新の情報が含まれています。これを使用して、Cisco Secure Workload はソフトウェアパッケージに既知の情報セキュリティの脆弱性があるかどうかを確認します。脆弱性が検出されると、シビラティ（重大度）と影響スコアを含む、すべての詳細を見つけることができます。その後、パッチの適用と計画の目的で、同じバージョンのパッケージがインストールされているすべてのサーバーをすばやく見つけることができます。セキュリティ運用担当者は、特定の脆弱性のあるパッケージがインストールされている場合にはホストを隔離するなど、特定のアクションを含むポリシーを事前定義できます。

製品の詳細

Q. Cisco Secure Workload プラットフォームは、強力なポリシーモデル内で許可ルールとブロックルールを組み合わせることができる許可リストセキュリティモデルを使用して柔軟なセグメンテーションを提供します。ブロックリストモデルと許可リストモデルにはどのような違いがありますか。

A. ブロックリストモデルと許可リストモデルには次のような違いがあります。

- **ブロックリスト：**名前によって悪意のある人物を識別します。その人物が中に入ることはできません。デフォルトでは、リストに名前がない人物であれば誰でも中に入ることができます。これは、長年使用されている従来のセキュリティモデルです。
- **許可リスト：**リストに名前があり、信頼できる人物以外は、誰も中に入ることはできません。

Q. 許可リストモデルの方が優れているのはなぜですか。

A. 許可リストモデルは、提供する権限アクセスを最小限にして環境内のラテラルムーブメントを制限するために、特定のアプリケーション要件に従ってモデル化された詳細なポリシーに基づいてプロアクティブな保護を提供します。ゼロトラストモデルには、許可リストポリシーが必要です。

Q. マイクロセグメンテーション ポリシーはどこで適用しますか。

A. マイクロセグメンテーション ポリシーは、定義されたポリシーに従ってラテラルムーブメントを制限するために、ワークロード内かワークロードのできるだけ近くで適用する必要があります。Cisco Secure Workload での適用には、主に、ワークロードのオペレーティングシステムに展開されたエージェントを介してワークロードのオペレーティングシステムのファイアウォール機能が使用されます。これらのエージェントにより、Linux ベースのサーバー（Kubernetes ノードを含む）では IP セットと iptables、Microsoft Windows サーバーでは Windows Filtering Platform（WFP）または Windows Advanced Firewall（WAF）セキュリティ機能を使用してポリシーが調整されます。また、セキュリティグループ（エージェント展開の有無にかかわらず）、およびアクセス コントロール ポリシー（ACP）とダイナミックオブジェクトを介した Cisco Secure Firewall を介した配信に対し、ポリシーが AWS との統合を通じて一貫して適用されます。ポリシーは、F5 および Citrix とのネイティブ統合を通じて ADC で適用できるほか、Cisco Secure

Workload のセキュアな Kafka ポリシーストリームによるオーケストレータ統合を通じてサードパーティのファイアウォール インフラストラクチャで適用することもできます。

Q. ポリシーはアプリケーション環境の変化に応じて動的に更新されますか。

A. Cisco Secure Workload は、豊富なコンテキストデータを使用して、インベントリ内のすべてのワークロードとエンドポイントのコンテキストステータスを継続的に追跡して更新します。Cisco Secure Workload ポリシーはコンテキストによるインベントリの照合に基づいて自然言語の形式で記述されており、継続的にすべてのワークロードのポリシーが自動で動的に更新されます。たとえば、特定のアプリケーション コンポーネントのインスタンスが追加されると、Cisco Secure Workload はそれらのインスタンスに同じポリシーを自動的に適用し、ワークロードの変化に適応するように関連するすべてのポリシーグループを更新します。また、ワークロードが移動するとポリシーも一緒に移動するため、管理者による追加のアクションは必要ありません。

Q. ポリシー違反が検出されたときに Cisco Secure Workload プラットフォームは通知を送信できますか。

A. はい。Cisco Secure Workload は、複数のメカニズムによるノースバウンド通知をサポートしています。Kafka、syslog、電子メールなどを使用できます。ノースバウンドシステムはこの通知を受け取って追加アクションを実行できます。たとえば、セキュリティインシデント/イベント管理（SIEM）システムは、これらのイベントを受け取ってチケットを自動的に開くことができます。

Q. ソフトウェアの脆弱性が見つかった場合、Cisco Secure Workload を使用してアクションを実行できますか。

A. はい。管理者は、特定の脆弱性に関連するポリシーや脆弱性スコアに基づくポリシーを定義できます。Cisco Secure Workload は、基準を満たすすべてのサーバーまたは脆弱なシステムと通信するすべてのサーバーに、指定されたポリシーを自動的に適用します。

Q. テレメトリのキャプチャを有効にした場合、サーバーの CPU に対してどのような影響がありますか。

A. ソフトウェアセンサーは、自己モニタリング機能を備えており、貴重なサーバーリソースの潜在的な過剰消費を防ぐために CPU とメモリの使用率を制限するしきい値を設定可能なサービスレベル契約（SLA）を提供します。センサーが CPU のしきい値を超えると、エージェントの CPU 使用率が SLA しきい値の範囲内に戻るまで、データ収集に選択的フィルタが適用されます。

Q. ソフトウェアセンサーはどの OS バージョンでサポートされていますか。

A. サポートされているオペレーティングシステムの完全なリストについては、Cisco Secure Workload のプラットフォーム情報のページ（www.cisco.com/c/en/us/products/security/tetration/platform-info.html）を参照してください。

Q. Cisco Secure Workload テレメトリではネットワークトラフィックがどの程度生成されますか。

A. Cisco Secure Workload は、パケット自体ではなく、メタデータのみを収集します。したがって、帯域幅要件は非常に低くなります。エージェントの構成で高忠実度フロー（5 タプル）または会話のみ（4 タプル）のいずれかを選択することで、フローごとの豊富な詳細か詳細を少なくした会話のみのデータを収集できます。会話のみの場合、帯域幅のオーバーヘッドがさらに少なく、データ保持期間が長くなります。

Q. Cisco Secure Workload プラットフォームのセキュリティは万全ですか。

A. はい。Cisco Secure Workload プラットフォームでは、ゼロトラスト、SELinux 制御、証明書ベースの認証、および暗号化を内部的に使用して、クラスタ間とクラスタ内のすべての通信の安全性を確保しています。

Q. これは「オープン」プラットフォームですか。

A. Cisco Secure Workload は非常にオープンなプラットフォームです。

- Cisco Secure Workload プラットフォームではすべてのポリシーを公開できます（JSON、XML、または YAML）。
- REST API により、ノースバウンドシステムを通じて情報を照会できます。
- Kafka は多数のコンシューマに情報を公開するためのストリーミング インターフェイスを提供します。この「プッシュインターフェイス」により、ノースバウンドシステムで通知を受け取り、サードパーティのセキュリティ オーケストレーション システムで使用するセキュアなポリシーストリームを提供できます。

導入オプション、ライセンス、および価格設定

Q. Cisco Secure Workload プラットフォームにはどのような導入オプションがありますか。

A. Cisco Secure Workload プラットフォームには、オンプレミス導入と Software-as-a-Service（SaaS）の柔軟なオプションがあります。次の 3 つの導入オプションを利用できます。

- Cisco Secure Workload SaaS：Cisco Secure Workload ソフトウェアがクラウドで実行され、ソフトウェアサービスとして使用できます。このオプションでは、プラットフォームハードウェアの導入やメンテナンスが不要で、Cisco Secure Workload ソフトウェアを管理する必要もありません。この導入モデルは、数万のワークロードに拡張できます。
- Cisco Secure Workload-M（小型フォームファクタ）：この導入オプションは、サーバー 6 台と Cisco Nexus 9300 スイッチ 2 台で構成されます。このプラットフォームは、詳細なフローテレメトリで最大 5000 のワークロード、会話のみのフローテレメトリで最大 10,000 のワークロードをサポートします。
- Cisco Secure Workload プラットフォーム（大型フォームファクタ）：この導入オプションは、サーバー 36 台と Cisco Nexus 9300 スイッチ 3 台で構成されます。このプラットフォームは、詳細なフローテレメトリで最大 25,000 のワークロード、会話のみのフローテレメトリで最大 50,000 のワークロードをサポートします。

Q. Cisco Secure Workload SaaS にはどのようにして接続しますか。

A. Cisco Secure Workload アーキテクチャでは、オンプレミスまたはクラウドベースのワークロードやインフラストラクチャと Secure Workload SaaS プラットフォームの間のデータのやり取りと制御にセキュアな暗号化された接続を利用しています。接続は常に Secure Workload SaaS プラットフォームへのノースバウンドで確立され、アウトバウンド接続用にプロキシの使用がサポートされています。VPN は必要ありません。

Q. Cisco Secure Workload の価格設定のコンポーネントは何ですか。

A. Cisco Secure Workload の価格は、次の 2 つのコンポーネントで構成されています。

- **ソフトウェアライセンス：**ソフトウェアのソフトウェア サブスクリプション ライセンスです。期間は 1 年、3 年、または 5 年で、年払いと前払いのオプションがあります。ソフトウェアライセンスのオプションは、Cisco Secure Workload SaaS とオンプレミスの導入で共通です。ライセンスには次の 2 種類があります。
  - **ワークロードライセンス：** テレメトリデータの収集、分析、およびポリシーの適用が行われるワークロード相当（仮想マシン、ベアメタルサーバー、コンテナホスト、または仮想デスクトップ（VDI）インスタンス）の数に基づきます。
  - **エンドポイントライセンス：**Cisco AnyConnect または Cisco ISE を介してテレメトリまたはコンテキストが収集されるエンドポイントデバイスの数に基づきます。
- **ハードウェアプラットフォーム（オンプレミス導入オプションにのみ適用）：** お客様のデータセンター環境内で Cisco Secure Workload を提供するためにオンプレミスで展開するハードウェアベースのアプライアンスオプションです。

Q. どのようなお客様、ユーザー、購入者が対象となりますか。

A. Cisco Secure Workload は、ゼロトラストアーキテクチャとマイクロセグメンテーションの提供を担当する、あらゆる規模の組織のセキュリティアーキテクト、セキュリティ運用担当者、および基幹業務マネージャを対象としています。マイクロセグメンテーションは、多くのアプリケーションおよびセキュリティ アーキテクト チームにとって優先順位が高く、オンプレミスのデータセンター、コンテナ環境、およびパブリッククラウド全体で効果的なマイクロセグメンテーションと一貫したポリシーの適用が不可欠です。

エコシステム

Q. Cisco Secure Workload と AppDynamics® は補完関係にありますか。

A. はい。Cisco Secure Workload と AppDynamics は互いに補完関係にあります。AppDynamics は、アプリケーション パフォーマンス管理（APM）に重点を置いており、アプリケーション（Java、.NET、C# など）内のインストルメントを使用して、個々のアプリケーション トランザクションおよび関連するパフォーマンス測定指標をモニターします。Cisco Secure Workload は、ハイブリッドマルチクラウド環境全体で、エージェントベースとエージェントレスの両方のアプローチを通じてゼロトラストのセグメンテーションおよびその他のワークロードセキュリティ機能を提供するセキュリティ プラットフォームです。

Q. エコシステムの価値を教えてください。

A. Cisco Secure Workload プラットフォームは、幅広いセキュリティのユースケースに対して実用的なインサイトを提供します。エコシステムパートナーは、このプラットフォームからのポリシーの推奨事項を利用し、データセンターネットワーク内やデータセンターの境界でおおまかな適用を実施できます。また、REST API を通じて Cisco Secure Workload プラットフォームからのワークロードプロファイル情報を照会し、独自のロジックを実装することもできます。

Q. Cisco Secure Workload エコシステムにはどのような外部プラットフォームが含まれますか。

A. Cisco Secure Workload には、幅広いエコシステムパートナーが存在します。それらのパートナーは、ユースケースに基づいて次のカテゴリに分類されます。

- **コンテキスト交換：**VMware vCenter、Kubernetes、Openshift、ServiceNow、AWS リソースタグ、Infoblox、DNS サーバー
- **セキュリティ オーケストレーション：**Algosec、Tufin、Skybox
- **アプリケーション配信：**Citrix、F5

エコシステムパートナーの統合の詳細については、ソリューション概要ドキュメント（www.cisco.com/c/en/us/products/data-center-analytics/Secure Workload-analytics/solution-overview-listing.html）を参照してください。

ソリューションの導入とサービス

Q. オンプレミス導入でカスタマーサイトには何が提供されますか。

A.

- Cisco Secure Workload または Cisco Secure Workload-M（SFF）ソリューションのいずれかを導入する場合、お客様の施設への出荷前に、ラックへの設置、スタック構成、接続、および基本ソフトウェアのロードが行われます。お客様は、環境に関する基本的なセットアップ情報を提供し、セットアッププロセスを完了するためにシステムソフトウェアをインストールする必要があります。
- Cisco Secure Workload は、Cisco Unified Computing System™（Cisco UCS®）C シリーズ ラックサーバー上に構築され、統合された高性能ネットワーク用に Cisco Nexus 9300 スイッチが組み込まれています。
- お客様の環境への Cisco Secure Workload の統合、ゼロトラストの適用のためのセグメンテーションポリシーの開発/検出、より徹底したワークロードセキュリティ対策について、シスコサービスのエキスパートによるサポートが受けられます。
- Cisco Secure Workload 向け Cisco Solution Support では、シスコのテクノロジーとソリューションパートナーのテクノロジーの両方に対応する一元的なサポートを提供しています。このマルチベンダー ソリューションに関するサポートエクスペリエンスを合理化するために、ソフトウェア、ハードウェア、およびソリューションレベルのサポートが 1 つのサービスに統合されています。

Q. 現在、Cisco Secure Workload のお客様をサポートするために、どのようなシスコサービスを利用できますか。

A. 次のシスコサービスを利用できます。

- 組織がソリューションを最大限に活用できるように、Cisco Secure Workload にはソリューション サポートサービスが含まれています。
- お客様がソリューションを適切に利用（導入）できるように、Cisco Secure Workload QuickStart サービスが Cisco Secure Workload プラットフォームとともに提供されます。主な成果物としては、現状仕様のドキュメント、ポリシーやエンドポイントをまとめた運用ランブックなどがあり、このプラットフォームの機能を理解できるようにお客様企業のスタッフに専門知識を提供することも含まれます。

- また、Cisco Secure Workload のお客様には、Cisco Solution Support を通じて、ソリューションに重点を置いた専門知識に加え、シスコ製品とソリューションパートナー製品による問題の一元的な管理および解決が提供されます。Cisco Solution Support の特徴とメリットは次のとおりです。
  - 問題の発生場所に関係なく問題解決に対応する一括窓口。最初のお電話から問題の解決までのサポートが合理化されます。
  - ソリューションパートナーのサポートチームを含む組織的なサポートフレームワーク。サポートに関するやり取りの仲介が不要になります。
  - ソリューションレベルの専門知識。複雑な問題の解決までが迅速になります。
  - サービスの一元化。シスコのハードウェア、ソフトウェア、およびソリューションレベルのサポートが単一のサービスで提供されます。

Q. 初期導入の範囲を超える Cisco Secure Workload の専門知識を求めるお客様に、追加サービスを提供していますか。

A. はい。サブスクリプション期間を通じて導入、最適化、および運用を支援するシスコのカスタマーエクスペリエンス（CX）チームと連携できます。

シスコサービスのエキスパートは、ワークロードセキュリティに関する豊富な経験と技術の枠にとらわれない専門知識を有しており、Cisco Secure Workload のエンジニアリングチームとも連携しています。

チャネル （Channels）

Q. 誰が Cisco Secure Workload プラットフォームを販売できますか。

A. すべてのシスコパートナーが Cisco Secure Workload を販売できます。特定のシスコ認定テクノロジーパートナー（ATP）の要件はありません。

Q. パートナーは Cisco Secure Workload プラットフォームをどのようなお客様に勧めるべきですか。

A. Cisco Secure Workload は幅広いお客様に価値を提供します。対象となる業種には、金融、医療、防衛、インテリジェンスなど、セキュリティとコンプライアンスが重要な関心事項である業界が含まれますが、これらに限定されません。

購入方法

購入オプションを確認し、シスコの営業担当者に問い合わせるには、https://www.cisco.com/c/ja_jp/buy.html にアクセスしてください。

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

0821-2023-000-X